大学院　電気通信研究科　　士前期課程　　電子工学専攻　　専攻		
氏　　名	DO TOAN MINH	学籍番号：0632036
論　文　題　目	カオスを用いた画像暗号化に関する研究	

要　　旨

暗号化問題は，工学分野での実用上重要な問題を多く含む。90年代から、カオス論理に基づいて、情報セキュリテイ技術の応用が研究されてきた。一般に、ほとんどの従来方法はカオスシステム次元と暗号化鍵を複雑化させようという焦点で研究している。しかし、これらの方法は攻撃評価に関して安全性が弱いと言われている。また、ハードウエア設計することが大変難しい。この点を解決するために、本研究では、入力画像とカオス信号との排他的論理算を行う従来方法の代わりに、入力画像とカオス信号生成と秘密鍵を関係的に設定することができる暗号化方法を提案する。さらに、FPGAを用いてそのハードウエアを実装して評価を行った。

カオスの特性は、初期条件値に関する鋭敏な依存性があり、初期の微小な誤差が時間と共に急速に成長し続け、軌道の未来は予測不可能になる。そこで、システム定数と初期条件が安全鍵として採用された。暗号化には　Chen　微分方程式を使用してカオス信号を生成する。LFSR(Linear Feedback Shift Register)によって生成された値を用いて元画像の画素確率を選択し、その値をChen微分方程式の初期条件として暗号化鍵を出す。また、LFSRによって生成された値をメモリに格納し、暗号化鍵と暗号化したい画素の検索距離は暗号化値となる。

3.4Ghzの CPU と 1.2Gb のメモリのPCを用いた場合、 256 x 256 画素の多値画像の暗号化は 0.375 秒であった。また、統計分析、差分攻撃、線形攻撃分析、特別攻撃分析を行った結果、従来方法より安全であると確認できた。